

## CLAIMS

We claim:

1. A method of detecting intrusion attempts on a computing system, comprising the steps of:
  - 5           creating a first mapping profile of a valid password;  
              storing the mapping profile in memory;  
              creating a second mapping profile of an entered password;  
              calculating a profile score by comparing the first mapping profile to  
the second mapping profile;
  - 10           comparing the profile score to a threshold value; and  
              classifying the entered profile into one of two or more security  
classifications based upon the comparison between the profile score and the  
threshold value.
- 15       2. The method of claim 1, wherein at least one of the security  
classifications represents an intrusion attempt on the computing system.
3. The method of claim 1, wherein the first mapping step and the second  
mapping step each comprise the steps of:
  - 20           comparing successive characters of the respective password;  
              assigning a value to each pair of successive characters based upon a  
keyboard characteristic corresponding to the pair of successive characters; and  
              generating a password mapping for the respective password based  
upon the assigned values.

4. The method of claim 3, wherein the keyboard characteristic is the distance between keys of the keyboard representing the pair of characters.

5 5. The method of claim 3, wherein the keyboard characteristic is the likelihood that one of the pair of characters is typed on a keyboard when the other key of the pair is intended to be typed.

6. The method of claim 3, wherein the second mapping step further  
10 comprise the step of:

comparing the valid password to the entered password; and

determining when a pair of characters in the entered password are a transposition of a corresponding pair of letters in the valid password; and, when there is a transposition,

15 adjusting the profile score.

7. The method of claim 1, wherein the computing system is a personal computer.

20 8. The method of claim 1, wherein the computing system is a telephone voice response system.

9. A password protection system, comprising:  
a first mapping profile corresponding to a valid password;

a second mapping profile corresponding to an entered password;  
a profile score based upon a comparison of the first mapping profile  
and the second mapping profile;  
a threshold value; and  
5 two or more security classifications; and  
logic for assigning the profile score to one of the two or more security  
classifications based upon a comparison between the profile score and the  
threshold value.

10 10. The system of claim 9, wherein at least one of the security  
classifications represents an attempted intrusion.

11. The system of claim 9, wherein each of the first and second mapping  
are generated by comparing successive characters of the respective password,  
15 assigning a value to each pair of successive characters based upon a keyboard  
characteristic corresponding to the pair of successive characters, and generating the  
respective password mapping based upon the assigned values.

12. The system of claim 11, wherein the keyboard characteristic is the  
20 distance between keys of the keyboard representing the pair of characters.

13. The system of claim 11, wherein the keyboard characteristic is the  
likelihood that one of the pair of characters is typed on a keyboard when the other key  
of the pair is intended to be typed.

14. The system of claim 9, wherein the profile score is also based upon whether or not any two successive characters of the entered password are transpositions of two, corresponding characters of the valid password.

5

15. A computer program product for detecting intrusion attempts on a computing system, comprising:

a memory;

logic, stored on the memory, for creating a first mapping profile of a valid password;

10

logic, stored on the memory, for storing the mapping profile in a memory;

logic, stored on the memory, for creating a second mapping profile of an entered password;

15

logic, stored on the memory, for calculating a profile score by comparing the first mapping profile to the second mapping profile;

logic, stored on the memory, for comparing the profile score to a threshold value; and

20

logic, stored on the memory, for classifying the entered profile into one of two or more security classifications based upon the comparison between the profile score and the threshold value.

16. The computer program product of claim 15, wherein at least one of the security classifications represents an intrusion attempt on the computing system.

17. The computer program product of claim 15, wherein the first mapping step and the second mapping step each comprise:

5 logic, stored on the memory, for comparing successive characters of the respective password;

logic, stored on the memory, for assigning a value to each pair of successive characters based upon a keyboard characteristic corresponding to the pair of successive characters; and

10 logic, stored on the memory, for generating a password mapping for the respective password based upon the assigned values.

18. The computer program product of claim 17, wherein the keyboard characteristic is the distance between keys of the keyboard representing the pair of characters.

15

19. The computer program product of claim 17, wherein the keyboard characteristic is the likelihood that one of the pair of characters is typed on a keyboard when the other key of the pair is intended to be typed.

20 20. The computer program product of claim 17, wherein the second mapping step further comprises:

logic, stored on the memory, for comparing the valid password to the entered password; and

logic, stored on the memory, for determining when a pair of characters in the entered password are a transposition of a corresponding pair of letters in the valid password; and, when there is a transposition,

logic, stored on the memory, for adjusting the profile score.